Data processing device and method for operating same which prevents a differential current consumption analysis

Technical field

The invention relates to a method of operating a data processing device, notably a chip card, which includes an integrated circuit which carries out, in dependence on a clock signal, arithmetic operations, notably cryptographic operations, data input and data output as well as data transfer between registers of the integrated circuit as disclosed in the introductory part of Claim 1. The invention also relates to a data processing device, notably a chip card, which is specifically intended to carry out the method and includes an integrated circuit which executes arithmetic operations, notably cryptographic operations, in dependence on a clock signal, the integrated circuit including a processor with an associated first register and data inputs and outputs as disclosed in the introductory part of Claim 3.

State of the art

In many data processing apparatus provided with an integrated circuit, for example, cryptographic operations are carried out so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried out by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a chip card or IC card. Data or intermediate results used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

Arithmetic operations performed by the integrated circuit, for example in order to calculate cryptographic algorithms, involve the formation of logic combinations of operands or intermediate results. Depending on the technology used, such operations, notably the loading of empty or previously erased storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of the current consumption occurs when the value of a bit storage cell changes, i.e. when its value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the

Hamming weight of the operand (= number of bits having the value "1") written into the empty register. Analysis of this current variation could thus enable extraction of information concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. When several current measurements are performed on the data processing apparatus, adequate information could be extracted, for example in the case of very small signal variations. On the other hand, a plurality of current measurements could also enable a possibly required differentiation. This type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus. "Differential Power Analysis" thus enables the extraction of additional internal information of an integrated circuit beyond pure functionality.

From US 5 297 201 it is known to combine a high frequency radiating computer with a device which also radiates high frequency similar to that of the computer. Thus, an unauthorized third party can no longer decode the high-frequency radiation of the computer. Crypto analysis by a third party having direct access to the computer, however, cannot be prevented by this system.

WO 90/15489 describes a protected communication system in which dummy traffic or dummy transfers are produced so as to impede cryptographic analysis. Crypto analysis by a third party having direct access to the computer, however, cannot be prevented either by this system.

Implementation of the invention, object, solution, advantages

It is an object of the present invention to provide an improved method and an improved data processing device of the kind set forth which eliminate the described drawbacks and offer effective protection against "Differential Power Analysis".

This object is achieved by means of a method of the kind set forth which is characterized as disclosed in Claim 1, and by means of a data processing device of the kind set forth which is characterized as disclosed in Claim 3.

To this end, in conformity with the method of the kind set forth according to the invention the integrated circuit is controlled in such a manner that the execution of arithmetic operations on the one hand and the data input/output as well as the data transfer from one register to another or between registers on the other hand is executed in parallel in time.

This offers the advantage that the differential power analysis does not have any clue as to when an arithmetic operation ends or when reading out/writing of registers takes place or when data input/output takes place, because periods of time of the actual calculations as well as the data input and data output are disguised. Differential power analysis is thus significantly obstructed, because it is no longer possible to determine from the outside whether a real calculation takes place or an input/output operation.

In order to disguise the arithmetic operations as well as data inputs/outputs even further, in a further version of the method dummy calculations are performed by a processor of the integrated circuit directly before, during and/or directly after the data transfer between the registers of the integrated circuit, which dummy calculations act on random or predetermined data, and no data are written into registers of the integrated circuit.

A data processing device of the kind set forth according to the invention is provided with a second register which is connected to the first register and includes the data inputs and outputs, and a control unit is connected to the integrated circuit, the control unit being constructed in such a manner that it controls parallel operation in time of the registers for data input/output and data transfer between the registers on the one hand and arithmetic operations of the processor on the other hand.

This offers the advantage that the differential power analysis does not have any clue as to when an arithmetic operation ends or when reading-out/writing of registers takes place or when data input/output takes place, because periods of time of the actual calculations as well as the data input and data output are disguised. The second register enables input/output of data while the processor is active and possibly writes data into the first register or reads out data from the first register. Differential power analysis is thus significantly obstructed because, when the second register is suitably controlled, it is no longer possible to determine from the outside whether a real calculation takes place or an input/output operation.

The first register in an advantageous further embodiment of the data processing device is an operand register of the processor and/or the second register is an operand register for the data input/output.

Preferred description of the drawings

The invention will be described in detail hereinafter with reference to the accompanying drawings. Therein:

Fig. 1 shows a block diagram of a preferred embodiment of a data processing device according to the invention,

Fig. 2 shows a block diagram of an integrated circuit of the data processing device of Fig. 1,

Fig. 3 graphically illustrates the activity of the data processing device according to the invention as a function of time according to the present state of the art, and

Fig. 4 graphically illustrates the activity of the data processing device according to the invention as a function of time in accordance with the invention.

Preferred implementation of the invention

Fig. 1 shows a preferred embodiment of a data processing device 100 according to the invention which includes an integrated circuit 10, a register 12 with program access 14 and a control unit 16. Via the lead 18, the control unit 16 and the integrated circuit receive a clock signal 20 as shown in the Figs. 3 and 4. Via control leads 22, the control unit 16 controls the integrated circuit 10 which includes data inputs 24 and data outputs 26.

As is shown in Fig. 2, the integrated circuit 10 includes a processor 28, a first operand register 30 which is associated with the processor 28 and a second operand register 32 which is connected to the first operand register 30. The second operand register 32 isprovided with the data inputs 24 and the data outputs 26. The clock signal 20 (Figs. 3 and 4) is applied, via the lead 18, to the processor 28 as well as to the two operand registers 30 and 32. During the execution of calculations or operations by the processor 28, it reads out data from the first register 30 or writes a result of a calculation into the first register 30. A data exchange or a mutual transfer of data, referred to hereinafter as R2-1, takes place between the registers 30 and 32 when data is transferred from the second register 32 to the first register 30 or, referred to as R1-2, when data is transferred from the first register 30 to the second register 32. A control lead 22, originating from the control unit 16, is connected to the second register 32 for the purpose of control whereas a further control lead 22 is connected to the first register 30 for the purpose of control.

According to an article "Differential Power Analysis" published by Paul Kocher on the Internet under http://www.cryptography.com/dpa: not only the input/output signals are analyzed but also a current consumption I_a or voltage drops ΔU_a of a supply voltage U_a of the integrated circuit. The success of this method of analysis is dependent on whether a number N_A of analog ($I_a(t)$ or $\Delta U_a(t)$) signal variations S(k,t) in time can be measured with

$k = \{1,...,N_A\}$ different operands in such a manner that it is possible to form a sum of the form:

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k).S(k,t)$$

with the coefficients p(i,k), where $i = \{0,1, 2,...\}$. When different signal variations $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$ ... are observed at the same instant $t = t_1$, differential power analysis can be succesful only if the integrated circuit executes the same arithmetic operation with different operands $k = \{1,...,N_A\}$ at that instant, i.e. it must be possible to make the signal variations S(k,t) register exactly. This holds not only for the calculation itself, but also for the input and output of data.

The invention disguises the periods of time of the actual calculation as well as the periods of time of the data input or data output. When the second register 32 is suitably controlled, it can no longer be detected from the outside when an actual calculation or an input/output takes place. Differential power analysis is thus significantly obstructed. The integrated circuit 10 according to the invention is provided with the two operand registers 30 and 32. This enables input and output of data via the second operand register 32, having the data inputs 24 and data outputs 26, also while the processor 28 is active in executing calculations or operations while using the first operand register 30.

Fig. 4 illustrates a mode of operation of the data processing device 100 and shows the clock signal 20 and a mode of operation of the processor and the operand registers on a time base 34. The reference numeral 36 denotes a mode of operation in which the processor executes a calculation. The reference numeral 38 denotes a mode of operation in which a data input or data output takes place; the reference numeral 40 denotes a mode of operation in which a data transfer R1-2 takes place while the reference numeral 42 denotes a mode of operation in which a data transfer R2-1 takes place.

Fig. 3 shows, in the same way as Fig. 4, a mode of operation of a conventional data processing device. Therein, the input and output phases 38 precede and succeed, respectively, the actual calculation 36 in time. The phases with the calculations 36 and the input/output 38 can be readily identified by means of differential power analysis; it can notably be detected which inputs 38 takes place during a calculation 40 and what outputs 38 result.

In the mode of operation according to the invention as shown in Fig. 4, the control unit 16 disguises the calculations 36 as well as the data inputs/outputs 38, 40, 42 by

controlling the data flow of the two operand registers 30, 32 so as to be parallel in time with the calculations 36. Calculations 36 always take place. However, the copying actions R1-2 40 and R2-1 42 now determine whether a calculation 40 is dependent on the input 38 or produces an output 38. The calculations before R2-1 42 and after R1-2 40 are, for example, dummy calculations. Dummy arithmetic operations are calculation operations which act on predetermined input data or random input data, the result being rejected and not taken up in the results or input data for the actual arithmetic operations. Additional dummy inputs/outputs can be optionally provided. The dummy calculations as well as the dummy inputs/dummy outputs produce current or voltage variations which are very similar to those of the actual calculations and inputs/outputs.

The control unit 16, provided according to the invention for the protection of the integrated circuit 10 against differential power analysis, is aimed specifically at the input/output phases 38, 40, 42 of calculations 36 to be performed in the circuit elements 10 by way of digital, electronic signal processing, because inputs/outputs could also be analyzed by differential power analysis of the current consumption. Thus, for differential power analysis it is of interest to know when a calculation 36 starts or ends. It is exactly this information in the current consumption signal that is suppressed in the method and the device according to the invention.